UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/846,443	04/30/2001	Gregory G. Rose	QCPA454B1C1	5374

23696 7590 07/07/2005

Qualcomm Incorporated
Patents Department
5775 Morehouse Drive
San Diego, CA 92121-1714

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/846,443	ROSE, GREGORY G.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3 and 4* is/are rejected.

7)☒ Claim(s) *2* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received on 03 May 2005. No claims have been amended, added, or canceled. Claims 1-4 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 03 May 2005 have been fully considered but they are not persuasive.

Claims 1 and 4 were rejected under 35 U.S.C. 103(a) as being unpatentable over Arazi, US Patent 5206824, in view of Bianco et al, US Patent 5365588, and Falk, US Patent 5249144. Claim 2 was rejected under 35 U.S.C. 103(a) as being unpatentable over Arazi in view of Bianco and Falk, and further in view of Rose et al, US Patent 6560338. Claim 3 was rejected under 35 U.S.C. 103(a) as being unpatentable over Arazi in view of Bianco and Falk, and further in view of Bardell, Jr., US Patent 4959832.

In reference to independent Claim 1, in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Specifically, Applicant argues that Falk does not disclose performing a non-linear operation on a shifted plurality of bits; however, Falk was not relied upon to teach this limitation.

Further, Applicant argues that Bianco does not disclose performing a non-linear operation on a selected portion of a shifted plurality of bits, where the portion is selected so that pairwise distances between elements of the portion are distinct values, and that Bianco instead discloses performing the non-linear operation on random inputs. However, the Examiner respectfully disagrees. The Examiner believes that Bianco does indeed disclose performing a non-linear operation on a selected portion of a shifted plurality of bits (see column 3, lines 56-59, as cited by the Examiner, where sets of taps of the working register are explicitly selected, and where the working register is an LFSR, and the sets of taps correspond to output bits that were shifted by the LFSR). Further, the Examiner believes that the distances between pairs of elements must necessarily be distinct values, if the selected sets of output bits (the selected sets of taps) provide input to independent functions (column 3, lines 56-59).

Additionally, Applicant argues that none of the cited references disclose a linear feedback shift register that is structured in accordance with a recurrence relation. However, the Examiner notes that all LFSRs inherently are designed so that the sequence will eventually repeat; therefore, any LFSR is inherently structured in accordance with a recurrence relation.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arazi, US Patent 5206824, in view of Bianco et al, US Patent 5365588, and Falk, US Patent 5249144.

In reference to Claim 1, Arazi discloses a method for generating a non-linear output from a linear feedback shift register that includes shifting bits through the LFSR and performing modular multiplications on the bits (column 4, lines 49-53). However, Arazi does not disclose performing a non-linear operation on a selected portion of the shifted bits, nor does Arazi explicitly disclose implementing the modular multiplications using look-up tables.

Bianco discloses an encryption method that includes an LFSR, in which bits shifted by the LFSR are used as the inputs to non-linear functions (column 3, lines 23-28; see also Figure 1 where Working Register 70 is an LFSR and Output Functions 80A-80N are non-linear). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the non-linear functions in the method of Arazi, in order to make the encryption algorithm more robust and resistant to cryptanalysis (see Bianco, column 1, lines 37-39).

Bianco further discloses that the non-linear functions can be implemented using ROM as look-up tables (column 5, lines 3-24); however, Bianco does not explicitly disclose using the look-up tables to implement modular multiplication. Falk discloses an arithmetic logic unit (ALU) in which a look-up table can be used to perform modular arithmetic functions (column 4, lines 26-31). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the method of Arazi in view of Bianco by implementing the modular multiplication using look-up tables, in order to allow the combination of functions to perform modular arithmetic functions (see Falk, column 1, lines 53-60).

In reference to Claim 4, Bianco further discloses initializing the LFSR by adding a key to an element of the LFSR (column 4, lines 33-35, where a random sequence is loaded into the working register) and adding a second key to the LFSR for each frame of data (column 4, lines 8-19, where the content of the key register is combined with the output feedback before being input to each cell of the working register).

5. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Arazi in view of Bianco and Falk as applied to claim 1 above, and further in view of Bardell, Jr., US Patent 4959832.

Arazi in view of Bianco and Falk disclose everything as applied above to Claim 1; however, they do not explicitly disclose the use of a stuttering operation. Bardell discloses that stuttering can be used on the output of an LFSR (column 7, lines 43-60, where decimation reads on stuttering). Therefore, it would have been obvious to one of

ordinary skill in the art at the time the invention was made to modify the method as disclosed by Arazi as modified above by including the use of a stuttering operation, in order to produce the maximum number of distinct output patterns of the LFSR (see Bardell, column 7, lines 31-33).

Allowable Subject Matter

6. Claim 2 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

7. The following is a statement of reasons for the indication of allowable subject matter:

Claim 2 is directed to a method for generating a non-linear output from a linear feedback shift register, including the steps of shifting bits through the LFSR, performing modular multiplications, and performing a non-linear operation. Additionally, Claim 2 specifically defines the non-linear operation as $V_n = (S_n + S_{n+5}) \times (S_{n+2} + S_{n+12})$ defined over $GF(2^8)$. The closest prior art, Arazi in view of Bianco and Falk, disclose a similar method including the steps described above in reference to independent Claim 1. However, neither Arazi nor Bianco nor Falk explicitly discloses a non-linear operation as defined in Claim 2. Rose et al, US Patent 6560338, discloses a non-linear function defined as $V_n = (S_n + S_{n+5}) \times (S_{n+2} + S_{n+12})$ (column 11, equation 5) that is defined over $GF(2^8)$ and can be applied to the output of an LFSR to generate a stream cipher

(column 11, line 1); however, because the present application has an earlier effective filing date than the Rose reference, the Rose reference does not constitute prior art.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. US Patent 6510228, to Rose, the named Applicant of the present application, discloses a method for generating encryption stream ciphers using an LFSR and non-linear functions.

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137